THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of verifying a transaction over a data communication system between a first and second correspondent through the use of a certifying authority having control of a certificate's validity, said certificate being used by at least said first correspondent, said method comprising the steps of:

   a) one of said first and second correspondents advising said certifying authority that said certificate is to be validated;

   b) said certifying authority verifying the validity of said certificate attributed to said first correspondent;

   c) said certifying authority generating implicit signature components including specific authorization information;

   d) forwarding to said first correspondent at least one of said implicit signature components for permitting said first correspondent to generate an ephemeral private key;

   e) forwarding to said second correspondent at least one of said implicit signature components for permitting recovery of an ephemeral public key corresponding to said ephemeral private key;

   f) said first correspondent signing a message with said ephemeral private key and forwarding said message to said second correspondent and

   g) said second correspondent attempting to verify said signature using said ephemeral public key and proceeding with said transaction upon verification.

2. A method as defined in claim 1, wherein said second correspondent advises said certification authority that said certificate is to be validated upon receiving an initial message from said first correspondent.

3. A method as defined in claim 2, wherein said at least one of said implicit signature components is forwarded to said second correspondent by said certifying authority.

4. A method as defined in claim 3, wherein said at least one of said implicit signature components is forwarded to said first correspondent by said second correspondent.

5. A method as defined in claim 4, wherein said generated implicit signature components includes:

a) γ_i, where $\gamma_i = kP + rP$, and where k is a long term private key of said first correspondent, r is a random integer generated by said certification authority, and P is a point on a curve; and

b) s_i, where $s_i = r - c \cdot H(A_i, \gamma_i)$, and where c is a long term private key of said certifying authority, A_i includes at least one distinguishing feature of said first correspondent and said specific authorization information, and H indicates a secure hash function;

wherein said long term private key of said first correspondent is sent to said certifying authority prior to said verification transaction.

6. A method as defined in claim 5, wherein A_i, γ_i, and s_i are forwarded to said second correspondent and s_i is forwarded to said first correspondent.

7. A method as defined in claim 5, wherein said distinguishing feature is includes at least one of a name of said first correspondent, a telephone number of said first correspondent, and an address of said first correspondent.

8. A method as defined in claim 5, wherein said specific authorization information includes at least one of a time of said transaction and a date of said transaction.

9. A method as defined in claim 6, wherein said ephemeral private key is generated according to $a_i = k + s_i$, where a_i is said ephemeral private key.

10. A method as defined in claim 9, wherein said ephemeral public key is recovered according to $a_iP = \gamma_i - H(A_i,\gamma_i)\cdot cP$, where a_iP is said ephemeral public key and cP is said certifying authority's public key.

11. A method as defined in claim 10, wherein said certifying authority verifies the validity of said certificate attributed to said first correspondent by checking a list for determining if said certificate has been revoked.

12. A method as defined in claim 10, wherein said ephemeral private key is a transaction specific private key and said ephemeral public key is a transaction specific public key.

13. A method as defined in claim 2, wherein said first correspondent advises said certification authority that said certificate is to be validated.

14. A method as defined in claim 14, wherein said at least one of said implicit signature components is forwarded to said first correspondent by said certifying authority.

15. A method as defined in claim 14, wherein said at least one of said implicit signature components is forwarded to said second correspondent by said first correspondent.

16. A method as defined in claim 15, wherein said generated implicit signature components include:

a) γ_i, where $\gamma_i = kP + rP$, and where k is a long term private key of said first correspondent, r is a random integer generated by said certification authority, and P is a point on a curve; and

b) s_i, where $s_i = r - c\cdot H(A_i,\gamma_i)$, and where c is a long term private key of said certifying authority, A_i includes at least one distinguishing feature of said

first correspondent and said specific authorization information, and H indicates a secure hash function;

wherein said long term private key of said first correspondent is sent to said certifying authority prior to said verification transaction.

17. A method as defined in claim 16, wherein A_i, γ_i, and s_i are forwarded to said first correspondent, and A_i and γ_i are forwarded to said second correspondent.

18. A method as defined in claim 16, wherein said distinguishing feature is includes at least one of a name of said first correspondent, a telephone number of said first correspondent, and an address of said first correspondent.

19. A method as defined in claim 16, wherein said specific authorization information includes at least one of a time of said transaction and a date of said transaction.

20. A method as defined in claim 17, wherein said ephemeral private key is generated according to $a_i = k+s_i$, where a_i is said ephemeral private key.

21. A method as defined in claim 20, wherein said ephemeral public key is recovered according to $a_iP = \gamma_i - H(A_i,\gamma_i)\cdot cP$, where a_iP is said ephemeral public key and cP is said certifying authority's public key.

22. A method as defined in claim 21, wherein said certifying authority verifies the validity of said certificate attributed to said first correspondent by checking a list for determining if said certificate has been revoked.

23. A method as defined in claim 21, wherein said ephemeral private key is a transaction specific private key and said ephemeral public key is a transaction specific public key.

24. A method as defined in claim 15, wherein said generated implicit signature components include a parameter for indicating a predetermined permission for said first correspondent, said second correspondent granting access to said first correspondent according to said predetermined permission upon verification of said signature.

25. A method as defined in claim 15, wherein said generated implicit signature components include:

a) γ_A, where $\gamma_A = aP + c_A P$, and where aP is a long term public key of said first correspondent, c_A is a random integer generated by said certifying authority, and P is a point on a curve; and

b) s_A, where $s_A = h(\gamma_A \| A_i \| cP)c + c_A \pmod n$, and where A_i includes at least one distinguishing feature of said first correspondent, where c is a long term private key of said certifying authority, n is a large prime number, and h indicates a secure hash function.

26. A method as defined in claim 23, wherein γ_A and s_A are forwarded to said first correspondent, and A_i and γ_A are forwarded to said second correspondent by said first correspondent.

27. A method as defined in claim 25, wherein said distinguishing feature is includes at least one of a name of said first correspondent, a telephone number of said first correspondent, and an address of said first correspondent.

28. A method as defined in claim 25, wherein said specific authorization information includes at least one of a time of said transaction and a date of said transaction.

29. A method as defined in claim 26, wherein said ephemeral private key is generated according to $d = a + s_A$, where d is said ephemeral private key.

30. A method as defined in claim 29, wherein said ephemeral public key is recovered according to $Q_A = h(\gamma_A \| A_i \| Q_C)Q_C + \gamma_A$, where Q_A is said ephemeral public key and Q_C is said certifying authority's long term public key.

31. A method as defined in claim 30, wherein said certifying authority recertifies said certificate attributed to said first correspondent by changing said random integer, c_A.

32. A method as defined in claim 30, wherein said ephemeral private key is a transaction specific private key and said ephemeral public key is a transaction specific public key.

33. A method as defined in claim 15, wherein said generated implicit signature components include:

a) i, where i is a certification period;

b) s_A, where $s_{A_i} = r_i c + k_i + c_A \pmod n$, n is a large prime number, c is a long term private key of said certifying authority, c_A and k_i are random integers, and $r_i = h(\gamma_A \| A_i \| cP \| k_i P \| i)$, where A_i includes at least one distinguishing feature of said correspondent and said specific authorization information, P is a point on a curve, and h indicates a secure hash function;

wherein $\gamma_A = aP + c_A P$, and where aP is a long term public key of said correspondent and γ_A has previously been determined by said certifying authority and forwarded to said correspondent.

34. A method as defined in claim 33, wherein i and s_A are forwarded to said first correspondent, and A_i and γ_A are forwarded to said second correspondent by said first correspondent.

35. A method as defined in claim 33, wherein said distinguishing feature is includes at least one of a name of said first correspondent, a telephone number of said first correspondent, and an address of said first correspondent.

36. A method as defined in claim 33, wherein said specific authorization information includes at least one of a time of said transaction and a date of said transaction.

37. A method as defined in claim 34, wherein said ephemeral private key is generated according to $d_i = a + s_A$, where d_i is said ephemeral private key.

38. A method as defined in claim 37, wherein said ephemeral public key is recovered according to $Q_A = r_i Q_C + \gamma_A + Q_i$, where Q_A is said ephemeral public key, Q_i is said certifying authority's certification period public key, and Q_C is said certifying authority's long term public key.

39. A method as defined in claim 38, wherein said certifying authority recertifies said certificate attributed to said first correspondent for each certification period, *i*, by changing said random integer, k_i.

40. A method as defined in claim 38, wherein said ephemeral private key and said ephemeral public key have a predetermined period of validity.

41. A method as defined in claim 40, wherein said predetermined period of validity is one transaction.

42. A method as defined in claim 40, wherein said predetermined period of validity is a predetermined number of transactions.

43. A method as defined in claim 40, wherein said predetermined period of validity is a predetermined time period.

44. A method for certifying a correspondent through the use of a certifying authority having control of a certificate's validity, said method comprising the steps of:

a) said certifying authority generating a first random number have a value;

b) generating implicit signature components based on said first random number;

c) publishing a public key of said certifying authority for use in verifying said correspondent;

d) forwarding said implicit signature components from said certifying authority to said correspondent;

wherein said certifying authority recertifies said correspondent's certificate by changing said value of said first random number.

45. A method as defined in claim 44, wherein c_A is said first random number generated by said certifying authority and said implicit signature components include:

a) γ_A, where $\gamma_A = aP + c_A P$, and where aP is a long term public key of said correspondent and P is a point on a curve; and

b) s_A, where $s_A = h(\gamma_A \| A_i \| cP)c + c_A \pmod n$, and where c is a long term private key of said certifying authority, n is a large prime number, A_i is an identifier of said correspondent and includes at least one distinguishing feature of said correspondent, and h indicates a secure hash function;

46. A method as defined in claim 45, wherein said correspondent is recertified by forwarding said implicit signature components for said first random number having said changed value from said certifying authority to said correspondent.

47. A method as defined in claim 43, wherein said first random integer has said value for one certification period, said value being changed for other of said certifications periods.

48. A method as defined in claim 47, wherein k_i is said first random integer generated by said certifying authority for an *i*th certification period and said implicit signature components include:

c) *i*, where *i* is a current certification period;

d) s_A, where $s_{A_i} = r_i c + k_i + c_A \pmod{n}$, n is a large prime number, c is a long term private key of said certifying authority, c_A is a second random integer, and $r_i = h(\gamma_A \| A_i \| cP \| k_i P \| i)$, where A_i includes at least one distinguishing feature of said correspondent, P is a point on a curve, and h indicates a secure hash function;

wherein $\gamma_A = aP + c_A P$, and where aP is a long term public key of said correspondent and γ_A has previously been determined by said certifying authority and forwarded to said correspondent.

49. A method as defined in claim 48, wherein said published information further includes $k_i P$ and *i*.

50. A method as defined in claim 49, wherein said correspondent is recertified by forwarding said implicit signature components for said first random number having said changed value from said certifying authority to said correspondent.